Cassandra Crossing/Xz, Solarwinds e l'Armageddon prossimo venturo

(582)—Il sabotaggio della libreria Xz è stato sventato, ed ancora una volta i buoni hanno vinto. Ma siamo sicuri che altrove gli…

Cassandra Crossing/ Xz, Solarwinds e l'Armageddon prossimo venturo

Figure 1: Trinity Site explosion, 0.016 second after explosion, July 16, 1945. The viewed hemisphere's highest point in this image is about 200 meters high. This work is in the public domain in the United States because it is a work by an employee of the US Government Title 17, Chapter 1, Section 105 of the US Code.

(582)—Il sabotaggio della libreria Xz è stato sventato, ed ancora una volta i buoni hanno vinto. Ma siamo sicuri che altrove gli attacchi alla supply chain del software non siano riusciti senza che nessuno se ne sia accorto?

5 aprile 2024—La realtà costringe Cassandra a prolungare ulteriormente la serie "Fine del Mondo" perché nuovi, gravissimi indizi emergono riguardo al fatto che le armi per l'Armageddon informatico prossimo venturo continuano ad accumularsi.

E di nuovo, ventate di ottimismo, espresse anche da addetti ai lavori, si propagano in maniera tanto inesplicabile quanto pericolosa. Non certo per stupidità o per incompetenza; forse per desiderio di quieto vivere, forse per ingiustificato ottimismo.

Ma per poter esprimere compiutamente ed in maniera comprensibile la sua tesi, Cassandra è come al solito costretta a riavvolgere il nastro e narrare un po' di antefatti.

Per fortuna ci basta riavvolgere solo al 2003, anno in cui viene portato alla luce il tentativo di introdurre una backdoor addirittura nel kernel di Linux.

Un amministratore del repository dei sorgenti ufficiali si accorse che una modifica minima apportata ad una banale routine del kernel non appariva richiesta da nessuno. Cassandra non pretende che il C sia patrimonio dei suoi lettori, ma giusto al fine di illustrare la diabolicità della modifica, si tratta della variazione di un singolo carattere in una singola riga, cioè da

```
if ((options == (__WCLONE|__WALL)) && (current->uid == 0))
```

a

```
if ((options == (__WCLONE|__WALL)) && (current->uid = 0))
```

la mancanza dell'ultimo "=" faceva si che, ad esempio, qualunque utente avesse usato il comando "kill" con un parametro opportuno (un valore a 16 bit) si sarebbe trovato "promosso" a root, e quindi avrebbe potuto prendere il completo controllo del server.

La modifica fu annullata, l'infrastruttura dei server di compilazione fu piallata e ricostruita da zero, ed i sorgenti furono ricaricati da un backup.

Buoni 1, Cattivi 0.

Ma basta fare un avanti veloce al 2006 per trovare una ulteriore modifica diabolica nella libreria OpenSSL. Due semplici linee commentate diminuivano drasticamente l'entropia dell'RNG della libreria. Per farla anche qui semplice, facevano si che, ad esempio, il numero di differenti chiavi crittografiche generabili dalla libreria passasse da un valore praticamente infinito a 32767. Chi avesse conosciuto questo fatto e precalcolato le opportune chiavi avrebbe potuto forzare qualunque algoritmo crittografico che usasse OpenSSL (cioè praticamente tutti) con estrema facilità.

Quando il problema fu scoperto e prontamente risolto, i suoi effetti non cessarono subito. Infatti ci vollero oltre due anni perché la maggioranza delle chiavi "deboli", generate e diffuse per tutta internet venisse rimpiazzata, cosa che ha lasciato ulteriori due anni di tempo agli autori della malefatta per approfittare dei suoi effetti.

Questo evento fu così sentito dai cronisti dell'epoca che addirittura il fumetto XKCD gli dedicò un'arguta vignetta.

Ma andiamo avanti, perché purtroppo non c'è niente da ridere.

Ci fu chi disse Buoni 2—Cattivi 0 e palla al centro.

Del calcolo di questo punteggio, che è un po' il nocciolo del ragionamento di Cassandra, riparleremo alla fine di questa esternazione.

Arriviamo rapidamente al 2020; un gruppo di criminali informatici al soldo di uno stato nazione attacca la rete di un produttore di software per la sicurezza informatica, probabilmente già nel 2018. Dopo aver violato la rete altera i server che compilavano il software destinato ad essere spedito ai clienti, in modo che includesse una backdoor.

Non stiamo parlando di un software qualsiasi, Solarwinds è un sofisticato software per la sicurezza informatica, installato dalle più grandi organizzazioni con stringenti necessità di sicurezza, tra cui, ad esempio, una ventina di agenzie governative americane, fornitori di armamenti, grandi aziende informatiche e compagnia cantando. Si, anche in Italia.

L'aggiornamento automatico di Solarwinds aveva quindi installato automaticamente una backdoor che rendeva semplicissimo violare le reti che lo utilizzavano; in questo modo migliaia di reti iperprotette si sono improvvisamente aperte ai criminali informatici che ne hanno potuto abusare a piacimento per anni. Quando l'attacco fu scoperto (perché di attacco si tratta), il principale problema per le organizzazioni colpite fu di capire se erano o no state violate, perché gli attaccanti erano del tipo più pericoloso, quelli bravi, che non si fanno scoprire e che è difficilissimo trovare e scacciare.

E finalmente arriviamo al 2024, ad oggi, anzi a due settimane fa, ed all'attacco alla libreria Xz.

Un dipendente Microsoft che utilizzava OpenSSL (si, di nuovo lei) si accorge che la nuova versione ci mette 500 millisecondi in più a compere certe operazioni rispetto alla versione precedente. Siccome evidentemente nella sua vita non aveva di meglio da fare e giudicava importante questo problema, si mette a controllare i codici sorgenti per cercarne il motivo. Con suo stupore si accorge che la nuova versione della libreria OpenSSL contiene un file binario proveniente da un'altra libreria, per l'esattezza Xz che è la libreria che si occupa di comprimere e decomprimere i file; si, proprio quella con cui zippate i vostri PDF, che lo sappiate o meno.

Si accorge con orrore che questa modifica permette, a chi possiede certe chiavi crittografiche, di iniettare ed eseguire qualunque programma direttamente nel kernel del sistema operativo, e di far succedere qualsiasi cosa; dal prendere il controllo completo del sistema a distruggere rapidamente e completamente tutti i server compromessi.

L'analisi retrospettiva degli avvenimenti ha rivelato che due anni prima uno sviluppatore anonimo aveva iniziato a proporre modifiche alla libreria Xz, che erano ragionevoli e quindi erano state accettate del suo amministratore, e poi a farsi accettare come co-amministratore della libreria stessa. Aveva poi lentamente sovvertito il sistema di compilazione della libreria stessa, inserendovi il codice malevolo destinato a finire nella libreria OpenSSL, e contemporaneamente svolgendo una sofisticata azione di ingegneria sociale nei confronti di chi avrebbe potuto controllare le sue modifiche in modo tale che queste verifiche non fossero fatte.

Poi, quando la libreria infettata ha cominciato a propagarsi sui primi server, uno di essi è stato quello del benedetto dipendente Microsoft con tanto tempo libero, che non ringrazieremo mai abbastanza e che meriterebbe un monumento.

Se questo scarno riassunto non vi paresse abbastanza, potete divertirvi ascoltando questo podcast in cui due titani della scena hacker italiana degli anni '90 discutono, approfonditamente e scherzosamente, della faccenda, condividendo anche un giudizio ottimistico per il futuro.

Quindi Buoni 3—Cattivi 0 e palla al centro?

Bene, questa valutazione è quella che ha accompagnato questi terrificanti eventi, venuti alla luce sempre per fortuna, e prima che potessero causare danni catastrofici. In effetti Solarwind ha davvero causato danni economici rilevantissimi e danni derivanti da furti di dati e da attività spionistiche non precisabili, ma dovrebbe aver spinto la comunità informatica mondiale ad attivarsi contro questo nuovo tipo di attacchi informatici.

Quindi Buoni 4—Cattivi 0??

Ed arriviamo alle conclusioni, probabilmente ormai chiarissime ai 24 informatissimi lettori di Cassandra.

Per tutte le divinità mai adorate dagli umani, da Astarte a Zaratustra, inclusi Manitù, Cthulhu e Yog-Setoth, è possibile che nessuno pensi a tutti gli attacchi di questa portata che non sono mai stati rilevati? Quelli in cui nessun dipendente insonne è inciampato, che nessun amministratore di sistema curioso ha mai rilevato?

Ma davvero ci sono addetti ai lavori che credono che i buoni continuino a segnare e che i cattivi siano costretti nella loro metà campo?

Davvero qualcuno può pensare che gli stati-nazione, i produttori di armi, i grandi e piccoli gruppi criminali e le mafie non stiano accumulando, in grandi e piccoli arsenali, queste "modifiche" al software che fa funzionare il mondo, queste armi informatiche che talvolta sono state anche testate od utilizzate su scala ridotta o con conseguenze circoscritte (i nomi SQL Slammer e Stuxnet non vi dicono niente?).

Cassandra è sempre stata andreottiana nell'animo, e **mai come in questo caso sente il dovere di invitare gli ottimisti a riconsiderare le proprie posizioni, non per un principio di precauzione, ma per puro e semplice realismo**.

L'Armageddon della prima guerra informatica mondiale è certamente, e ripeto certamente in fase di avanzata realizzazione. Poi non dite che non vi avevo avvertito.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on April 5, 2024.

Canonical link

Exported from Medium on August 27, 2025.